Computer Networks & Software Inc.

Accelerating CNS

Security Considerations for the Future e-Enabled Aircraft

Chris A. Wargo

I-CNS Conference

April 30, 2002

7405 Alban Station Court, Suite B201, Springfield, Virginia 22150-2318 (703) 644-2103

www.cnsw.com

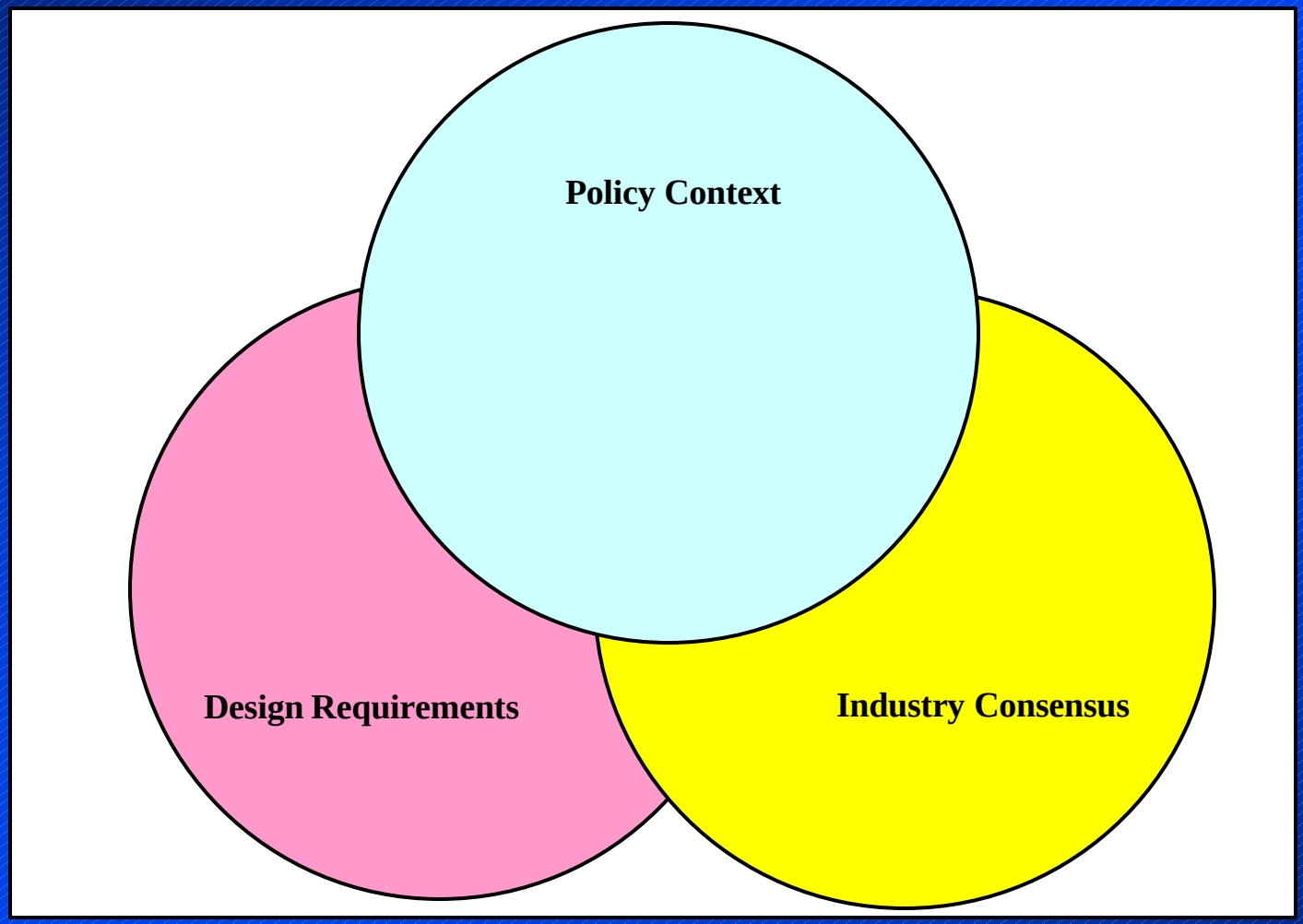
Agenda

Accelerating CNS

- **Overview/Issues**
- **Ongoing work of AEEC 664/628/763**
- **Next Steps**

Information Security Discussion

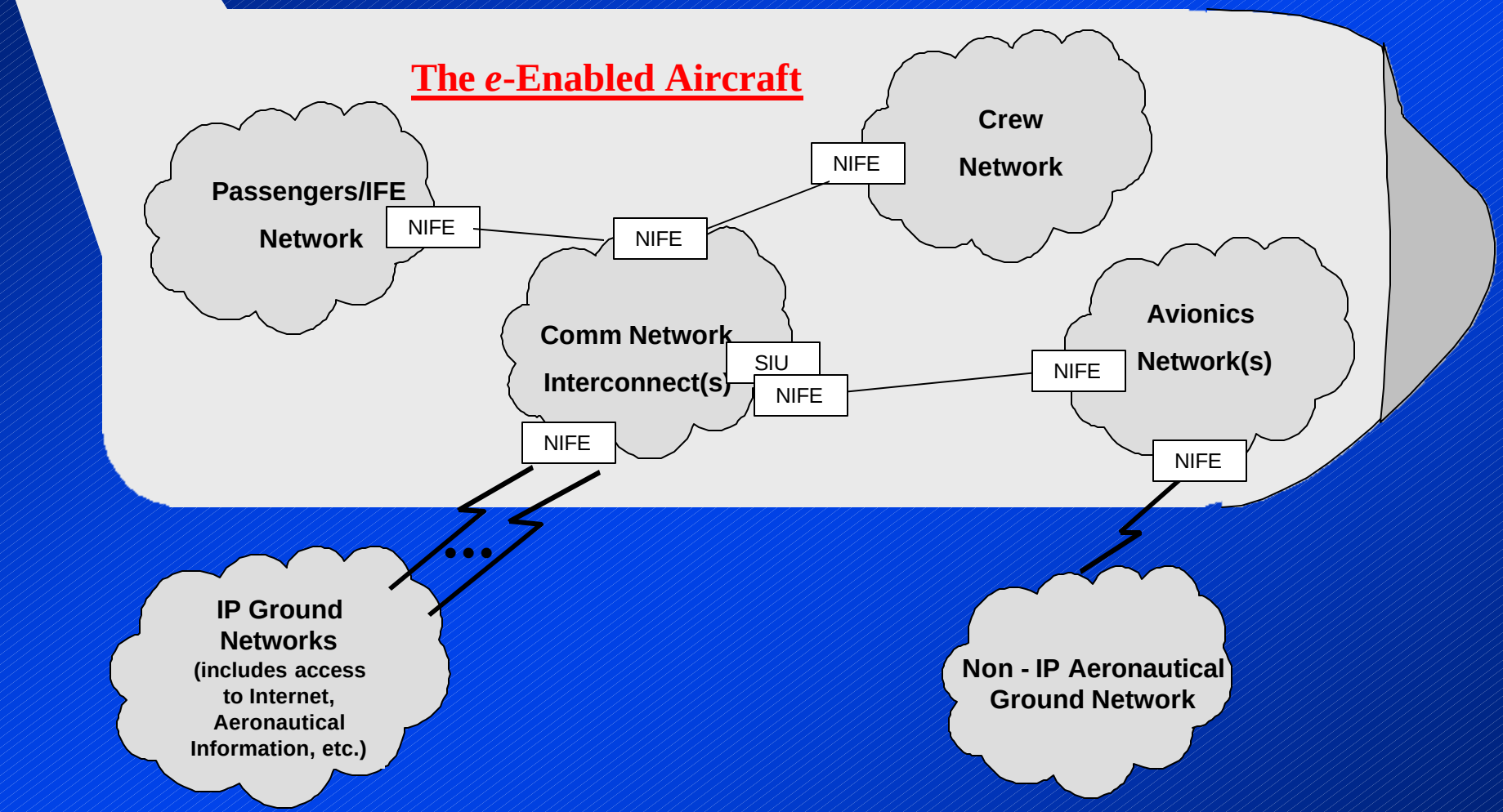
Accelerating CNS



The need is to develop the solution set

Reference Model – Domains

Accelerating CNS



Source: Developed ADN 664 Meeting 02/13/02

NIFE = Network Interface Function Element

SIU = Secure Interface Unit

What is Security?

Accelerating CNS

Not just a data link issue - security is not an add-on.

- **Technical**
  - **Functionality, Architecture, and Design**
- **Organizational**
  - **Definition, Separation, "Need to Know"**
- **Procedural**
  - **Identification, Authentication, Limitation, Observation**

Security must be built into the integrated network design.

Before Designing – Industry Consensus

Accelerating CNS

- **What is our obligation about security?**
- **What is our investment in security?**
- **How do we protect that investment?**
- **What is the right design?**

Need an industry policy covering not just one for ATC, but one covering all domains.

Develop the Policy

Accelerating CNS

- **Analyze the Required/Desired Capabilities**
  - **Cockpit, Cabin, Maintenance, Ground Crews**
- **Define Acceptable Operational Limits**
  - **Permissible Behavior in Failure or Attack Conditions**
- **Establish Integrated Security Policies**
  - **Policies Must Comprise All Operational Areas**

Vision

Accelerating CNS

- **Each constituent has multiple internal and external direct connections with the others and with the world – creating the air commerce web.**

E-Enabled Aircraft - Motivation

- **Business process integration**
- **Driven by passengers**
- **Use of mass market “open systems” products**
- **Lower development and operational costs**
- **Safety**

Reference Domains - Top Level

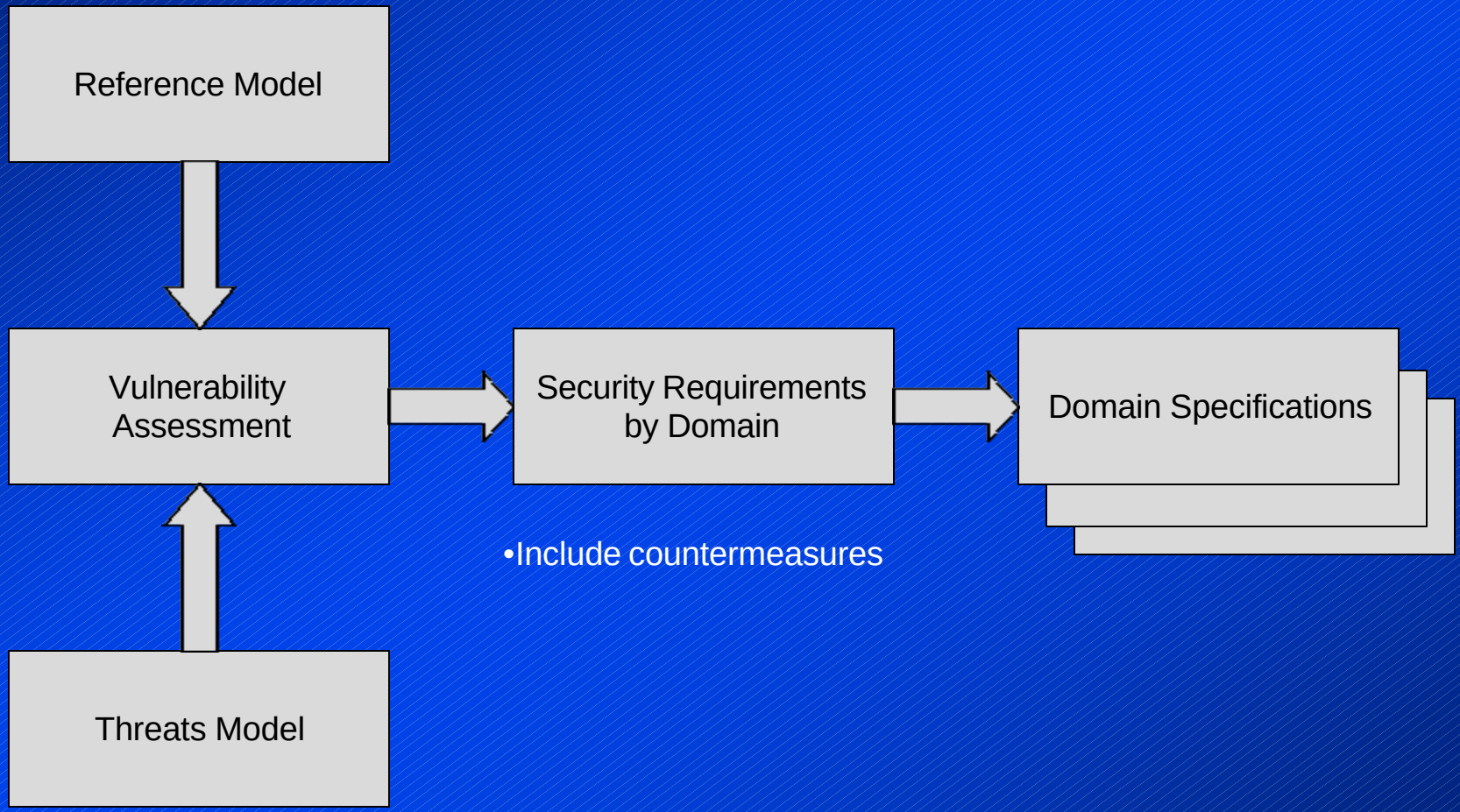
Accelerating CNS

- **Onboard**
  - **Communications Network Interconnect (AEEC 763)**
  - **Crew (Crew Information System)(AEEC 763/628)**
  - **Passenger/In-flight Entertain (IFE) (AEEC 628)**
  - **Avionics (multiple) (AEEC 664)**
- **Offboard**
  - **IP-Based - Internet/VPN**
  - **Non-IP Aeronautical**
- **Must look at the security from the context of all domains and cross domains both onboard and offboard.**
- **Must look at the dataflows between trusted areas.**

Typical Methodology

Accelerating CNS

•Consider all Domains



•Consider Targets

Threat Definitions

Accelerating CNS

Types of Threats

- Impact on life
- Impact upon property
- Impact on opportunity

Impact of Successful Threat Action

- Grave - loss of life or injury
- Critical - injury and serious damage to property
- Some - damage to present or future resources
- Annoyance - minimal loss of time, induces stress
- Little - minor disruption
- Unknown
- None

Example Attack Methods

- **Pre-production compromise (built-in back doors)**
- **Substitution of parts (Trojans in software)**
- **Code attacks (viruses)**
- **Network attacks (worms)**
- **Denial of Service attacks**
- **System specific attacks (OS vulnerability)**
- **Authentication bypass (theft of credentials, spoofing)**
- **Shutdown of support systems (power, AC, flight controls etc.)**
- **Disgruntled employee (malicious or paid)**

Threat Impacts

Accelerating CNS

	Success of Threat Action results in:			
Domain/Interface	Human User disruption or denial	Application Disruption or Failure	Network Disruption or Failure	End System Disruption or failure
Onboard				
Comm Network Interconnect	Up to critical	Some	Critical	Critical
Crew (non-pilot)	Some	Some	Critical	Critical
Passenger/ In-Flight Entertainment (IFE)	Annoyance	Annoyance	Revenue Related (Some)	Future Revenue (Some)
Avionics	Grave	Grave	Grave	Grave
Offboard				
IP-Based ▪ Aeronautical (non ATC)/VPN ▪ Internet	Critical Annoyance	Some Annoyance	Critical Annoyance	Critical Annoyance
Aeronautical Non IP-Based	Grave	Critical	Critical	Critical
Interfaces (cross-domain)				
IP GN to Comm Net Interconnect	Up to critical	Up to critical	Up to critical	Up to critical
Non-IP AG to Avionics	Up to grave	Up to grave	Up to grave	Up to grave
IP GN Internet to Passenger/IFE	Some	Some	Some	Some
CNI to Avionics	Grave	Grave	Grave	Grave
CNI to Crew	Critical	Some	Some	Some
CNI to Passengers/IFE	Some	Some	Some	Some
Passenger/IFE to Avionics	Annoyance	Annoyance	Annoyance	Annoyance
Crew to Avionics	Critical	Some	Some	Some

Network Security Services/Functions

Accelerating CNS

- **F1: Authentication**
- **F2: Access**
- **F3: Data Confidentiality**
- **F4: Data Integrity**
- **F5: Non-Repudiation**
- **F6: Intrusion Protection Methods**
- **F7: Counter Measures**
- **F8: Recovery of System/Operation**
- **F9: Logging**

Network Security Sub-functions

Accelerating CNS

- **F1: Authentication**
  - **F1.1: Validity Checking**
  - **F1.2: Protection of Stored Validity Data**
  - **F1.3: Confidentiality of Data in Transit**
  - **F1.4: Additional Security Measures**
- **F2: Access**
  - **F2.1: Access Control**
  - **F2.2: Access List Administration**
- **F3: Data Confidentiality**
  - **F3.1: Encryption**
  - **F3.2: Key Distribution and Management**
  - **F3.3: Level of Security**
  - **F3.4: Layer of Encryption (Physical, Network, Higher)**

Security Sub-functions (cont..)

- **F4: Data Integrity**
  - **F4.1: Acceptable transmission error**
  - **F4.2: Anti-Spoofing/Message Digests**
- **F5: Non-Repudiation**
  - **F5.1: Confirmation**
  - **F5.2: Retention of Confirmation**
- **F6: Intrusion Protection Methods**
  - **F6.1: Bastion Host**
  - **F6.2: Filters**
  - **F6.3: Application Gateway (Proxy Server)**
  - **F6.4: Internal Domain Name Server (DNS)**

Security Sub-functions (cont..)

- **F7: Counter Measures**
  - **F7.1 Protection**
    - » Denial of service, code (virus), network (worms), Trojan software
  - **F7.2 Detection**
  - **F7.3 Response**
- **F8: Recovery of System/Operation**
  - **TBD**
  - **TBD**
- **F9: Logging**
  - **TBD**

Assessment Matrix (Key Dataflows)

Accelerating CNS

Security Function/ Sub-function	Aero IP GN To CNI	Internet To IP GN To CNI	CNI to Passengers /IFE	CNI to Crew.	CNI to Avionics	Aero Non IP GN To Avionics
F1 Authentication						
F1.1 Validity Checking	Offboard	Offboard	Yes + Billing	Yes	Yes, Might be static	Offboard
F1.2 Protection of Stored Data	Yes	User Defined	User defined	Yes	Yes	Yes
F1.3 Confidentiality of data in transmit	Yes	User defined	User defined	Yes	Yes (AG Appls)	Yes
F1.4 Additional Security Measures	Maybe	No	No	No	Maybe	Maybe
F2 Access Control						
F2.1 Control	Yes	Yes	Yes	Yes	Yes	Yes
F2.1 Access List Admin	Yes	Yes	Yes	Yes	Yes	Yes
F3 Data Confidentiality						
F3.1 Encryption	Yes	User Defined	User defined	Yes	Yes	Yes
F3.2 Key Distribution and Management	Yes	User defined	User defined	Yes	Yes	Yes
F3.3 Level of Security	Yes	No	No	No	Yes	No

Assessment Matrix (Key Dataflows)

Accelerating CNS

Security Function/ subfunction	Aero IP GN to CNI	Internet to IP GN to CNI	CNI to Passengers /IFE)	CNI to Crew	CNI to Avionics	Aero Non IP GN to avionics
F3.4 Layer of encryption						
F3.4.1 Physical	No	No	No	No	No	No
F3.4.2 Network	Yes	User defined	Yes	Yes	Yes	Yes
F3.4.3 Higher Layers	No	User defined	User defined	No	No	Yes
F3.5 Encryption API.	TBD	No	TBD	TBD	TBD	TBD
F4 Data Integrity						
F4.1 Acceptable Transmit Error	Yes	User defined QoS	Yes	Yes	Yes	Yes
F 4.2 Anti spoofing	Yes	No	No	Yes	Yes	Yes
F5 Non - repudiation						
F5.1 Confirmation	Yes	User defined	No	Yes	Yes	Yes
F5.2 Retention of confirmation	Yes	User Defined	No	Yes	Yes	Yes

Assessment Matrix (Key Dataflows)

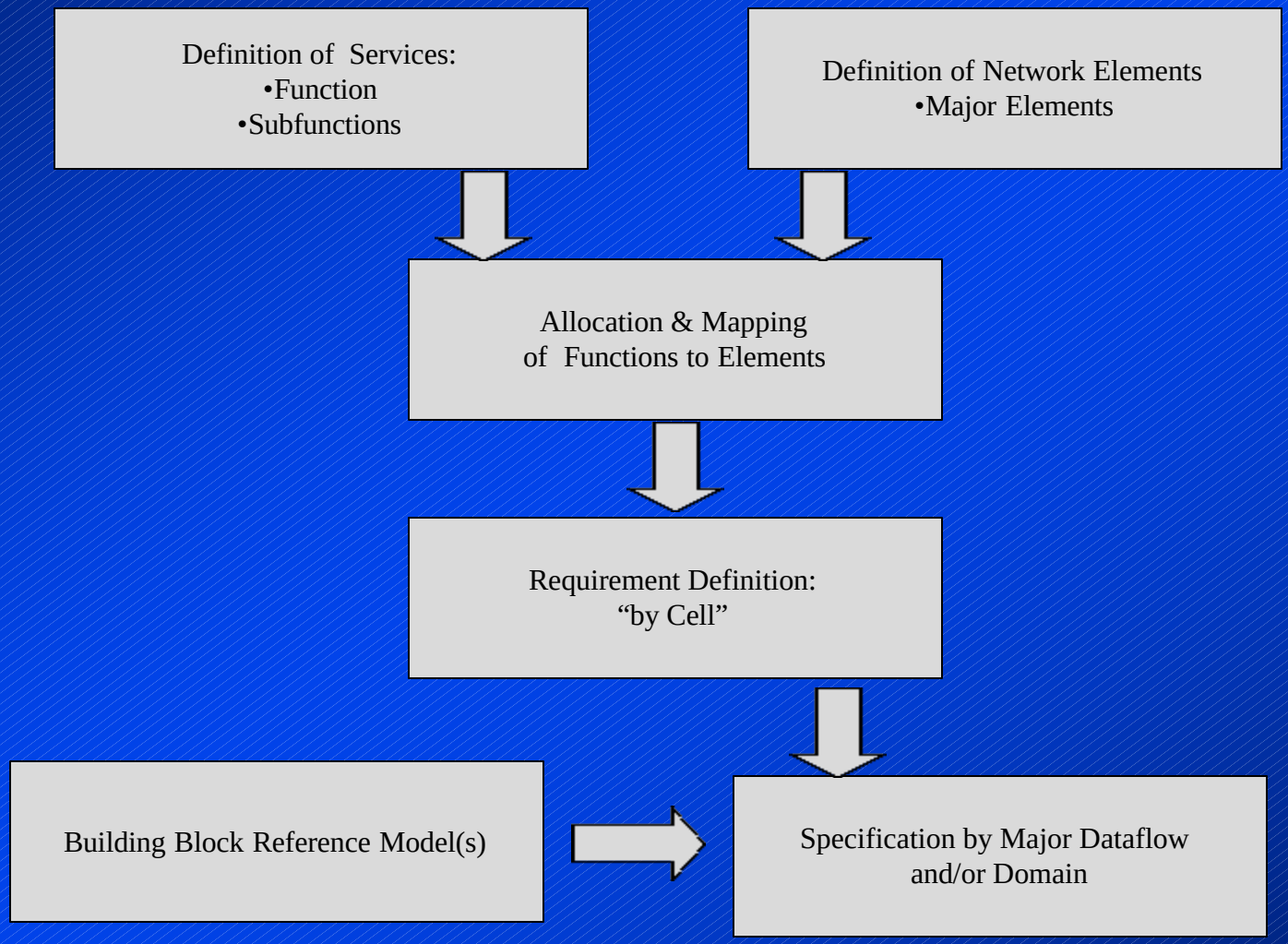
Accelerating CNS

Security Function/ subfunction	Aero IP GN to CNI	Internet to IP GN to CNI	CNI to passrs/IFE	CNI to Crew	CNI to Avionics	Aero Non IP GN to Avionics
F6 Intrusion Protection Methods						
F6.1Bastion Host	No	No	No	No	No	No
F6.2 Filters	Yes	Yes	Yes	Yes	Yes	Yes
F6.3 Proxy Server	No	No	No	Yes	No	Yes
F6.4. Internal DNS	No	No	No	No	No	Yes
F7 Counter measures						
F7.1 Protection						
F7.1.1 Denial of Service	Yes	No	No	Yes	Yes	Yes
F7.1.2 Code (virus)	Yes	Yes	Yes	Yes	Yes	Yes
F7.1.3 Network (worms)	Yes	Yes	Yes	Yes	Yes	Yes
F7.1.5 Trojan Sw	Yes	No	No	Yes	Yes	Yes
F7.2 Detection	Yes	Yes	Yes	Yes	Yes	Yes
F7.3 Response	Yes	Yes	Yes	Yes	Yes	Yes
F8 Recovery	Yes	No	No	Yes	Yes	Yes
F9 Logging	No	No	Yes	Yes	Yes	Yes

Internetworking Architecture Analysis

Accelerating CNS

Detailed Methodology



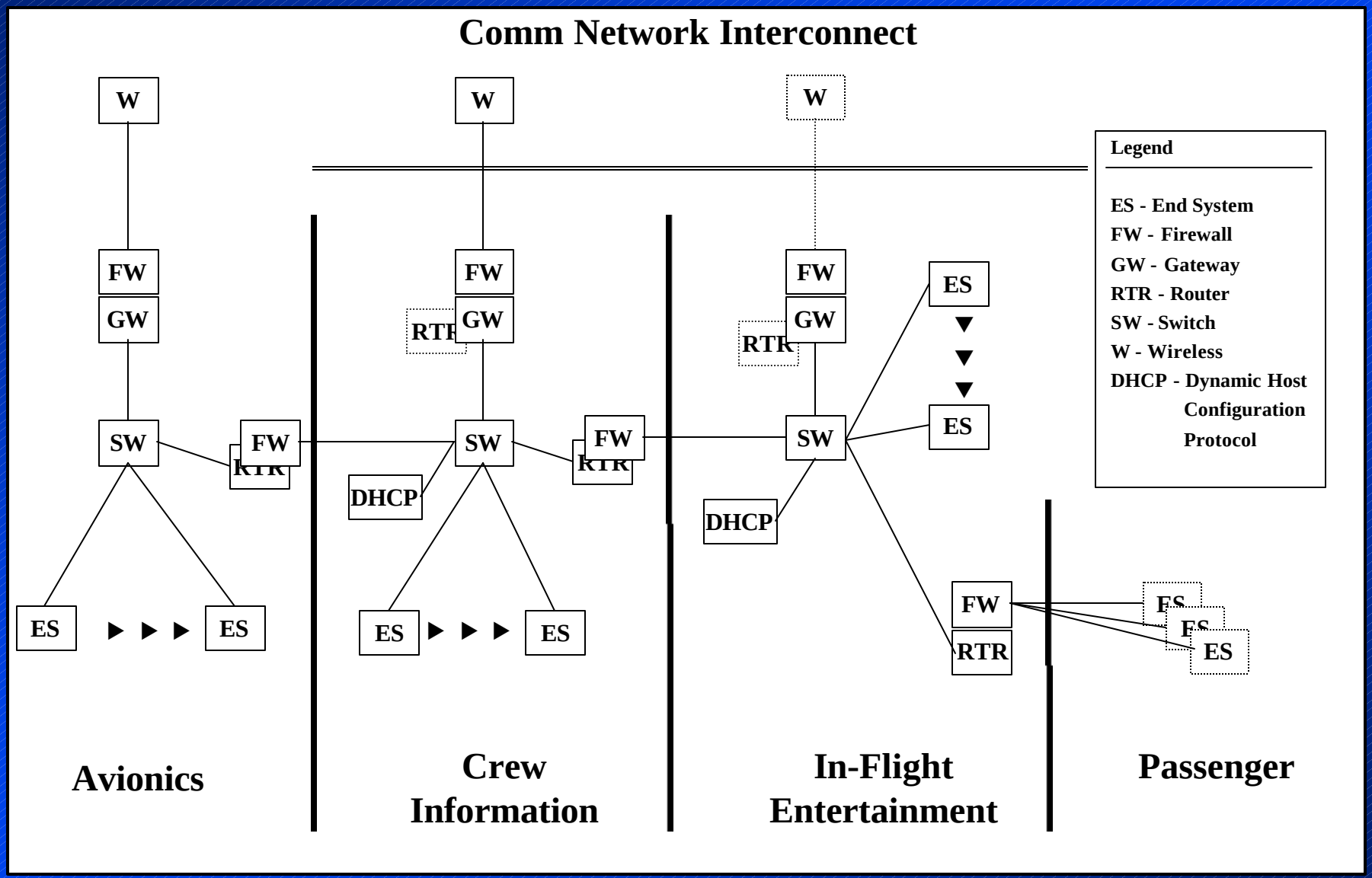
Building Block Reference Model

Accelerating CNS

- **View each domain as a set of Network Functional Elements (NFEs).**
- **Analyze the dataflows between domains.**
- **Specify the requirements for the services performed by each NFE in the dataflow between trusted areas.**
- **Understand the operational impacts and costs.**

Building Block Reference Model

Accelerating CNS



Network Security Functional Elements

Accelerating CNS

	Authentication	Access	Data Confidentiality	Data Integrity	Non-Repudiation	Intrusion Protection Methods	Counter Measures	Recovery of System / Operation	Logging
End System (or DTE)	●	●	●	●	●	●	●	●	●
Autoconfigure / Loader	-	-	-	-	-	-	-	-	-
Certification Authority	●	-	●	●	●	-	-	-	●
DHCP	-	-	-	●	-	-	-	-	○
DNS	○	-	-	●	-	●	-	-	○
Network Management Station	●	●	●	●	●	-	-	-	●
Firewall	●	●	⊙	●	⊙	●	●	-	●
Gateway	⊙	●	⊙	●	⊙	●	●	-	○
Router	⊙	●	⊙	●	⊙	●	●	-	○
Access Point	⊙	⊙	●	⊙	⊙	⊙	-	-	-
Bridge (or Switch)	⊙	⊙	⊙	⊙	⊙	⊙	-	-	●
Backbone	○	○	⊙	⊙	⊙	⊙	-	-	-
Cable Plant	⊙	⊙	⊙	⊙	⊙	⊙	-	-	-
Repeater (or Hub)	⊙	⊙	⊙	⊙	⊙	⊙	-	-	-

Legend	Meaning
-	Not Applicable
○	Optional
⊙	Present, but not required for a special task
●	Present, required for a special task

Security Sub-functions – Authentication

Accelerating CNS

F1: Authentication	*F1.1: Validity Checking*	*F1.2: Protection of Stored Validation Data*	*F1.3: Confidentiality of Data in Transit*	*F1.4: Additional Security Measures*
End System (or DTE)	●	●	●	○
Certification Authority	●	●	●	○
Network Management Station	●	●	●	○
Firewall	-	-	●	-

Legend	*Meaning*
-	Not Applicable
○	Optional
⊙	Present, but not required for a special task
●	Present, required for a special task

Security Sub-functions – e.g.,Authentication

Accelerating CNS

F1: Authentication	*F1.1: Validity Checking*	*F1.2: Protection of Stored Validation Data*	*F1.3: Confidentiality of Data in Transit*	*F1.4: Additional Security Measures*
End System (or DTE)	Shall require valid UserID/Password combination to access Network services.	May store passwords locally; if so, these passwords shall be stored in an encrypted format.	Shall encrypt sensitive information (e.g. passwords) before transmitting through the network.	May employ additional security measures (e.g. smart cards, single-use passwords).
Certification Authority	Shall validate credentials before performing services for a user.	May store passwords and private keys locally; if so, these shall be stored in an encrypted format.	Shall encrypt sensitive information (e.g. passwords, private keys) before transmitting through the network.	May employ additional security measures (e.g. smart cards, single use passwords).
Network Management Station	Shall require valid UserID/Password combination to access the system.	May store passwords locally; if so, these shall be stored in an encrypted format.	Shall encrypt sensitive information (e.g. passwords) before transmitting through the network.	May employ additional security measures (e.g. smart cards, single use passwords).
Firewall	-	-	Shall apply filters to prevent sensitive data from crossing into publicly accessible domains.	-

Next Steps

- **Break down the End-to-End communications process by potential information flow and describe what services are required for each flow (see reference model).**
- **Potential endpoints to consider include IP and Non-IP Ground systems, the Avionics and Pilot, the Crew, and the Passengers**
  - **Ground IP Avionics**
    - AOC, Weather
  - **Ground Non-IP Avionics**
  - **Avionics Crew**
  - **Ground IP Crew**
  - **Ground IP Passenger**

Next Steps – Example

Accelerating CNS

	F1: Authentication	*F3: Data Confidentiality*	*F4: Data Integrity*
Ground IP → Avionics	●	●	●
Ground Non-IP → Avionics	●	●	●
Avionics → Crew	●	●	●
Ground IP → Crew	○	○	●
Ground IP → Passengers	-	○	●

Legend	*Meaning*
-	Not Applicable
○	Optional
⊙	Present, but not required for a special task
●	Present, required for a special task

Next Steps – Example

Accelerating CNS

F5: Data Integrity	*F4.1: Acceptable Transmission Error*	*F4.2: Anti-Spoofing / Message Digests*
Ground IP → Avionics	●	●
Ground Non-IP → Avionics	●	●
Avionics → Crew	●	○
Ground IP → Crew	●	○
Ground IP → Passengers	●	○

Legend	*Meaning*
-	Not Applicable
○	Optional
⊙	Present, but not required for a special task
●	Present, required for a special task

Next Steps – Example

Accelerating CNS

F5: Data Integrity	*F5.1: Acceptable Transmission Error*	*F5.2: Anti-Spoofing / Message Digests*
Ground IP → Avionics	Checksums and CRC algorithms shall be used to achieve error free transmission.	Essential IP communications shall be validated through message digests.
Ground Non-IP → Avionics		Essential Non-IP communications shall be validated through message digests.
Avionics → Crew		Communications between the avionics and the crew may be validated through message digests. If any commands are sent from the crew to the avionics, these shall be validated through message digests.
Ground IP → Crew		Communications between the crew and Ground IP systems may be validated through message digests. Essential communications should not go through this channel.
Ground IP → Passengers		Communications between the passengers and Ground IP systems may be validated through message digests. This is left to individual passengers to implement as required.

The Approach Summary

Accelerating CNS

- **Need to develop a clear threat assessment.**
- **Need to develop AEEC Network Security Policy that is applicable to all domains.**
- **Develop specific security design**
  - **Separate security domains onboard**
  - **Relative levels of security per domain**
  - **Functional limitation between domains**
  - **Definitive operational predetermination**
  - **Define procedural and administrative rules**

Contacts

Computer Networks & Software, Inc.

7405 Alban Station Ct.
Suite B-201
Springfield, VA 22150-2318

CNS: Chris Dhas or Chris Wargo
703-644-2103
Chris.Dhas@CNSw.com, Chris.Wargo@CNSw.com
www.CNSw.com